Sandy Bacik

From: Sandy Bacik
Sent: Friday, January 20, 2012 6:39 AM
To: csctgarchi@nist.gov; Tillman, Leonard
Subject: CSWG Architecture minutes from 20120119

CSWG Architecture twiki: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi
Chair: Sandy Bacik (sandy.bacik@enernex.com)

20120119 Minutes

1. Conceptual security architecture - applying security services (http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/20120112-SecurityServices.ppt).
   a. We continued work on reviewing the service definitions and if the security service should be applied at the enterprise level, component level, application level, and to ALL messages.
   b. A "Yes" or "Required" means the service would need to be defined and applied at each C-I-A level and a "No" or "Optional" means the service is not necessarily defined but may be changed to a "Yes" based on the C-I-A level.
   c. We discussed combining the "Enterprise Registration" and "Enterprise Unique Naming" services, because the base definitions are very similar. Consensus was to keep them separate, because Enterprise Registration is a superset of Enterprise Unique Naming.
   d. We discussed removing the "Directory Service" service, because this would really be a specific technology that would be implemented and this should not be at the conceptual level. The consensus was to keep it, because it can be applied as a service across many types of systems.
   e. We discussed and had consensus on merging "Integrity Protection - Hardware", "Integrity Protection - Message", "Integrity Protection - Software", and "Integrity Protection - Stored Data" services into one superset security service of "Integrity Protection".
      i. NOTE: We will need to revisit the same type merging with the confidentiality services.
   f. We discussed and had consensus on changing “Trusted Time” to “Time Synchronization”.
   g. Incident Response: Enterprise, SG Component, SG Application, all messages - Yes.
   h. Incident Reporting: Enterprise, SG Component, SG Application, all messages - Yes.
   i. Intrusion Detection: Enterprise, SG Component, SG Application - Yes; all messages - No.
   j. Message Replay Protection: Enterprise - No; SG Component, SG Application, all messages - Yes.
   k. Non-Repudiation: Enterprise, SG Component, SG Application, all messages - Yes.
   l. Personnel Security: Enterprise, SG Component, SG Application - Yes; all messages - No.
   m. Physical Security: Enterprise, SG Component - Yes; SG Application, all messages - No.
   n. Replication and Backup - Data: Enterprise, SG Component, SG Application, all messages - Yes.
   o. Replication and Backup - Software: Enterprise, SG Component, SG Application - Yes; all messages - No.
   p. Risk Management - Data: Enterprise, SG Component, SG Application, all messages - Yes.
   q. Security Alarm Management - Software: Enterprise, SG Component, SG Application - Yes; all messages - No.
   r. Security Measurement and Metrics: Enterprise, SG Component, SG Application - Yes; all messages - No.
   s. Security Monitoring: Enterprise, SG Component, SG Application - Yes; all messages - No.
   t. Security Operations Management: Enterprise, SG Component, SG Application - Yes; all messages - No.
   u. Security Policy Management: Enterprise, SG Component, SG Application - Yes; all messages - No.
   v. Security Provisioning: Enterprise, SG Component, SG Application, all messages - Yes.
   w. Security Service Management: Enterprise, SG Component, SG Application, all messages - Yes.
   x. Security Training and Awareness: Enterprise, SG Component, SG Application - Yes; all messages - No.
   y. Software Licensing: Enterprise, SG Component, SG Application - Yes; all messages - No.
   z. System Audit: Enterprise, SG Component, SG Application, all messages - Yes.
   aa. System Configuration Protection: Enterprise, SG Component, SG Application - Yes; all messages - No.
   bb. Time Synchronization: Enterprise, SG Component, SG Application, all messages - Yes.
2. Attendees

a. Daniel Friedman
b. Elizabeth Sisley
c. Leonard Tillman
d. Neil Greenfield
e. Sandy Bacik
f. T.N. Choubey

Regards,
Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant
EnerNeX
p: 865.696.4470
e: sandy.bacik@enernex.com // www.enernex.com